Configuration.zipファイルを使用したFMTからFMCへのFDMの移行

内容

はじめに

このドキュメントでは、FMTを使用してFMCに移行するSecure Firewall Device Manager(FDM)の設定file.zipを生成する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シスコファイアウォール脅威対策(FTD)
- Cisco Firewall Management Center(FMC)
- ファイアウォール移行ツール(FMT)
- Postman APIプラットフォーム

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

FTD7.4.2

FMC 7.4.2

FMT 7.7.0.1

ポストマン11.50.0

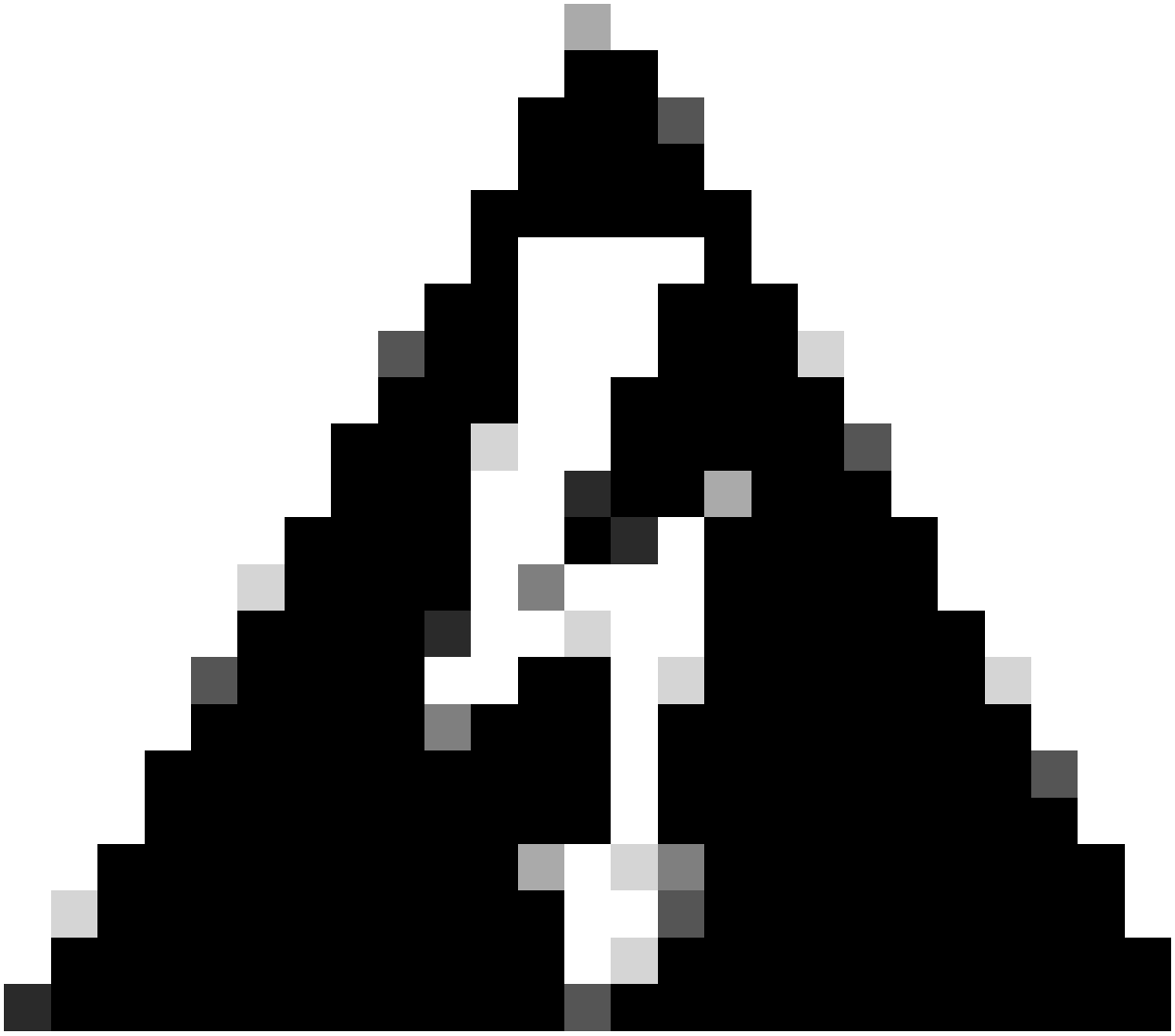
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

- FDMは、さまざまな方法でFMCに移行できます。このドキュメントでは、API要求を使用してコンフィギュレーション.zipファイルを生成し、そのファイルを後でFMTにアップロードしてコンフィギュレーションをFMCに移行するシナリオについて説明します。
- このドキュメントに示す手順ではPostmanを直接使用するため、Postmanをインストールしておくことをお勧めします。使用するPCまたはラップトップは、FDMおよびFMCにアクセスできる必要があります。また、FMTがインストールされ、実行されている必要があります。

考慮事項

- このドキュメントでは、FMTでの使用よりも多くの設定.zipファイルの生成に焦点を当てています。
- 構成.zipファイルを使用したFDM移行は、非ライブ移行用であり、宛先FTDがすぐに必要になることはありません。

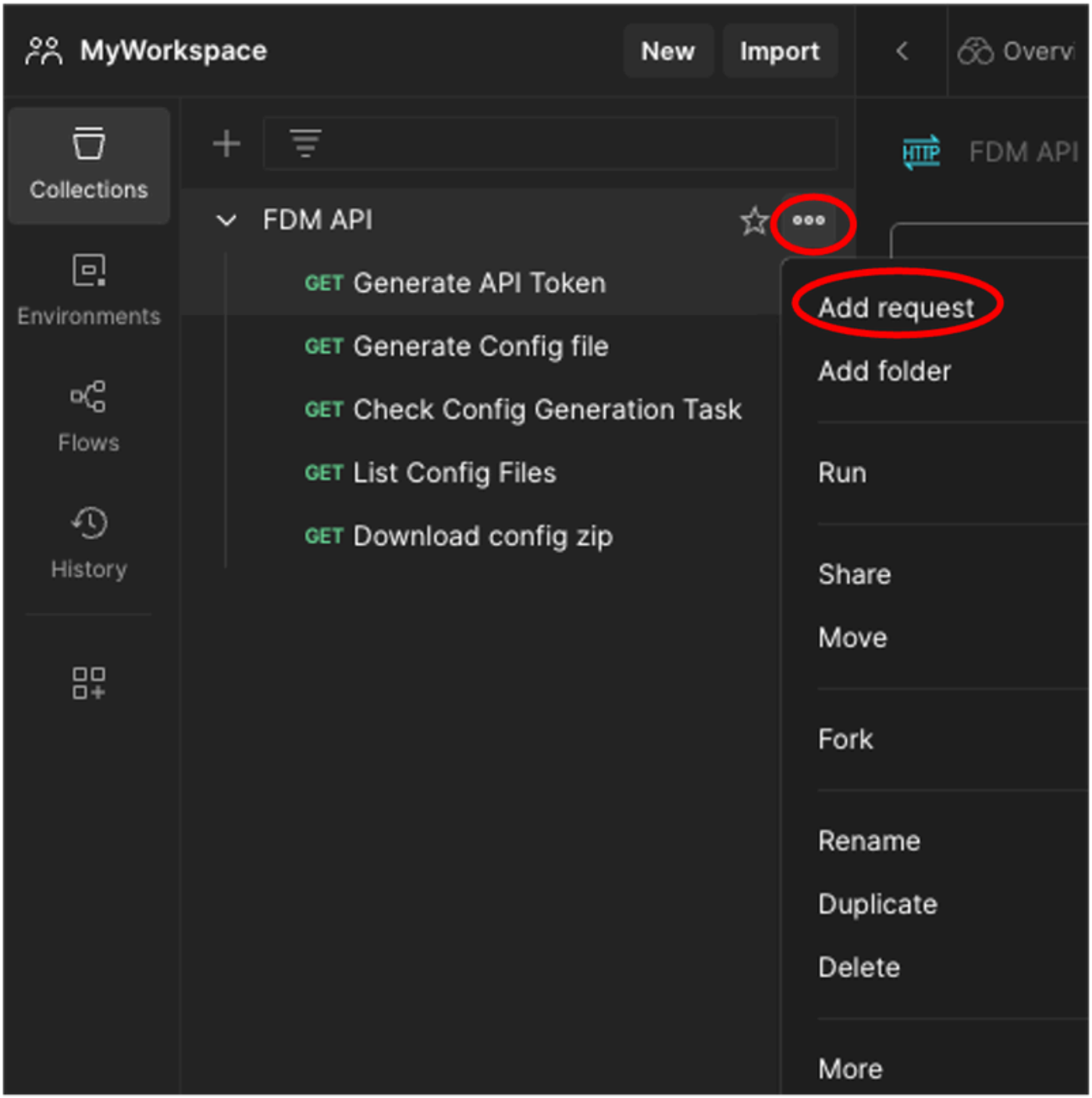


警告：このモードを選択すると、では、アクセスコントロールポリシー(ACP)、ネットワークアドレス変換ポリシー(NAT)、およびオブジェクトのみを移行できます。移行するオブジェクトに関しては、ACPルールまたはNATでそれらのオブジェクトを使用する必要があり、そうでない場合は無視されます。

コンフィギュレーション

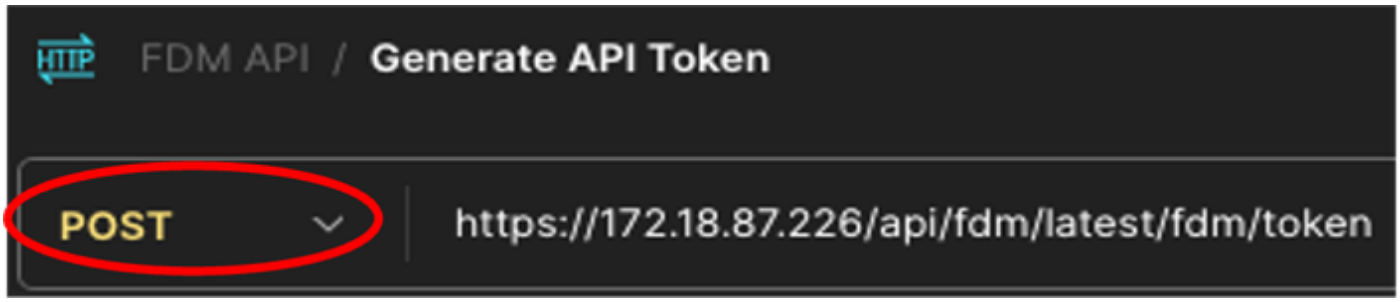
API要求 – Postman

1. Postmanで新しいコレクションを作成します（このシナリオではFDM APIが使用されます）。
2. 3つのドットをクリックし、Add requestをクリックします。



Postman – コレクションの作成と追加の要求

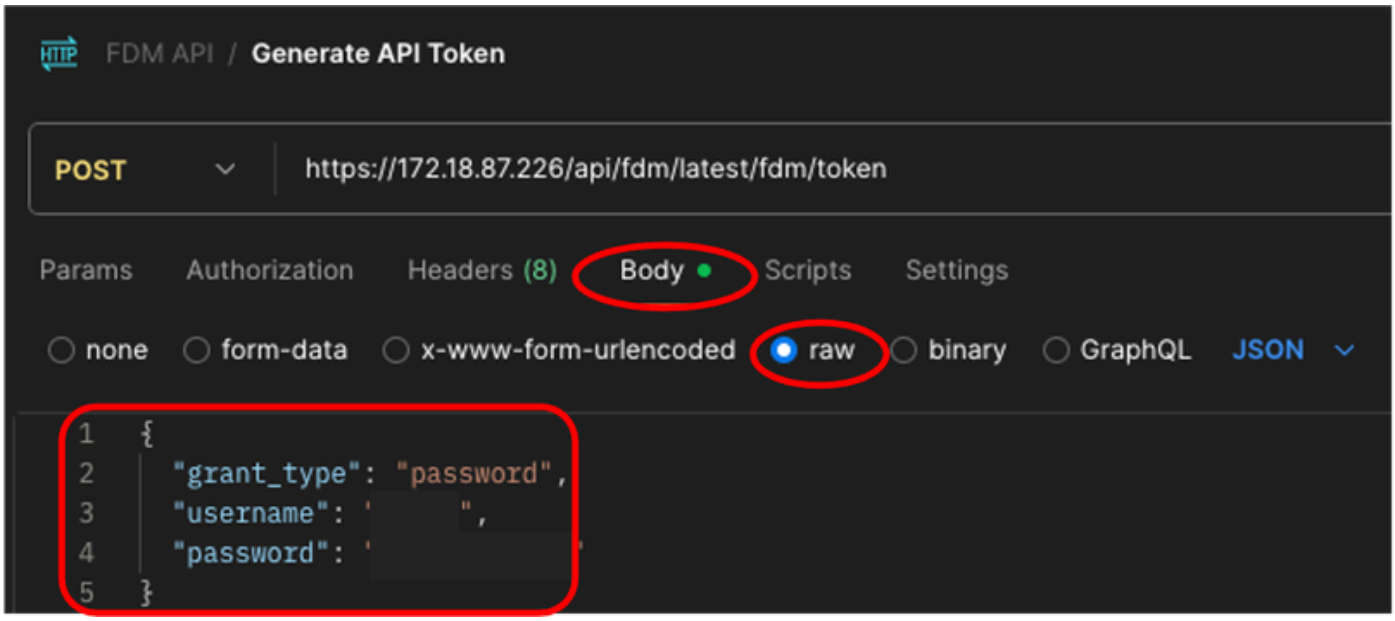
3. この新しい要求を呼び出します： APIトークンを生成します。これはGET要求として作成されますが、この要求を実行するときには、ドロップダウンメニューからPOSTを選択する必要があります。POSTの横のテキストボックスに、次の行https://<FDM IP ADD>/api/fdm/latest/fdm/tokenを挿入します



Postman：トークン要求

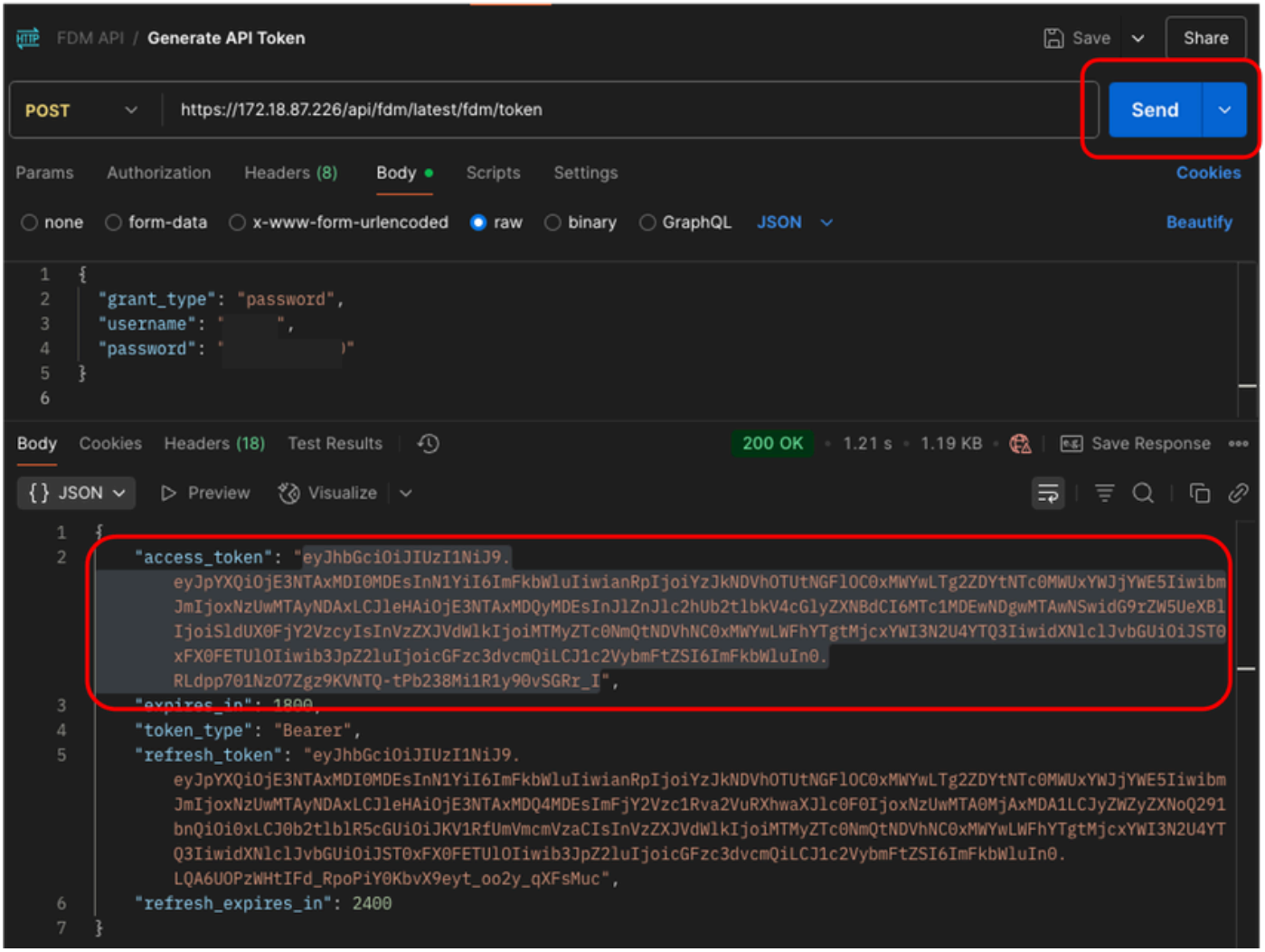
4. 「本体」タブで「raw」オプションを選択し、このフォーマットを使用してFTD(FDM)デバイスにアクセスするための「資格証明」を入力します。

```
{
   "grant_type": "password",
   "username": "username",
   "password": "password"
}
```



Postman – トークン要求本文

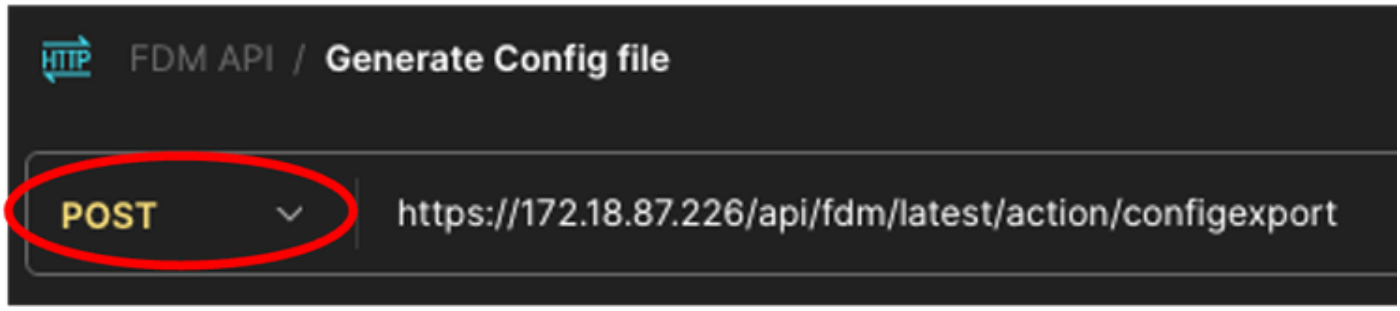
5. 最後に、Sendをクリックしてアクセストークンを取得します。問題がなければ、200 OKの応答を受信します。トークン全体のコピーを作成します（ダブルクォート内）。これは、後の手順で使用します。



Postman – トークンが正常に生成されました

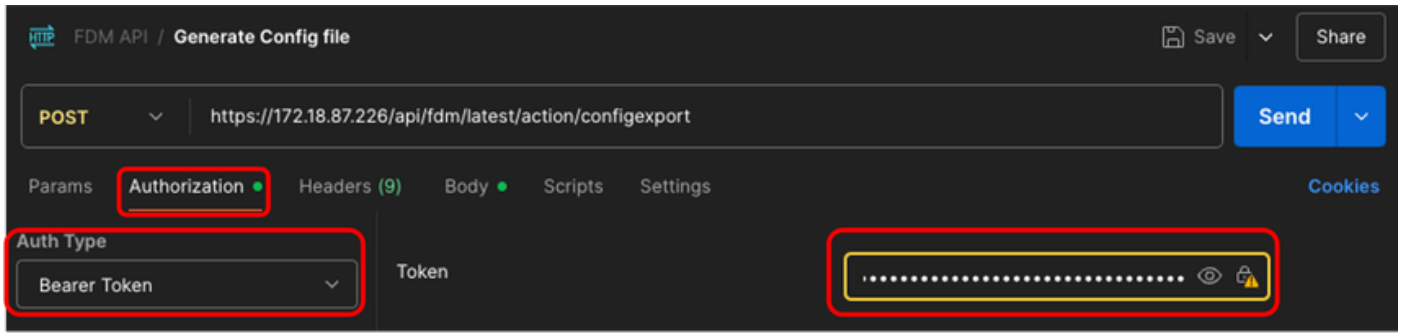
6. ステップ2を繰り返して新しい要求を作成し、POSTを再度使用します。

7. この新しい要求を「構成ファイルの生成」と呼びます。これはGET要求として作成されますが、この要求を実行するときには、ドロップダウンメニューからPOSTを選択する必要があります。POSTの横のテキストボックスに、次の行https://<FDM IP ADD>/api/fdm/latest/action/configexportを挿入します



Postman – 構成ファイル要求の生成

8. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスにステップ5でコピーしたトークンを貼り付けます。



Postman – 構成ファイルの生成要求 – 承認

9. 「本体」タブで「raw」オプションを選択し、この情報を入力します。

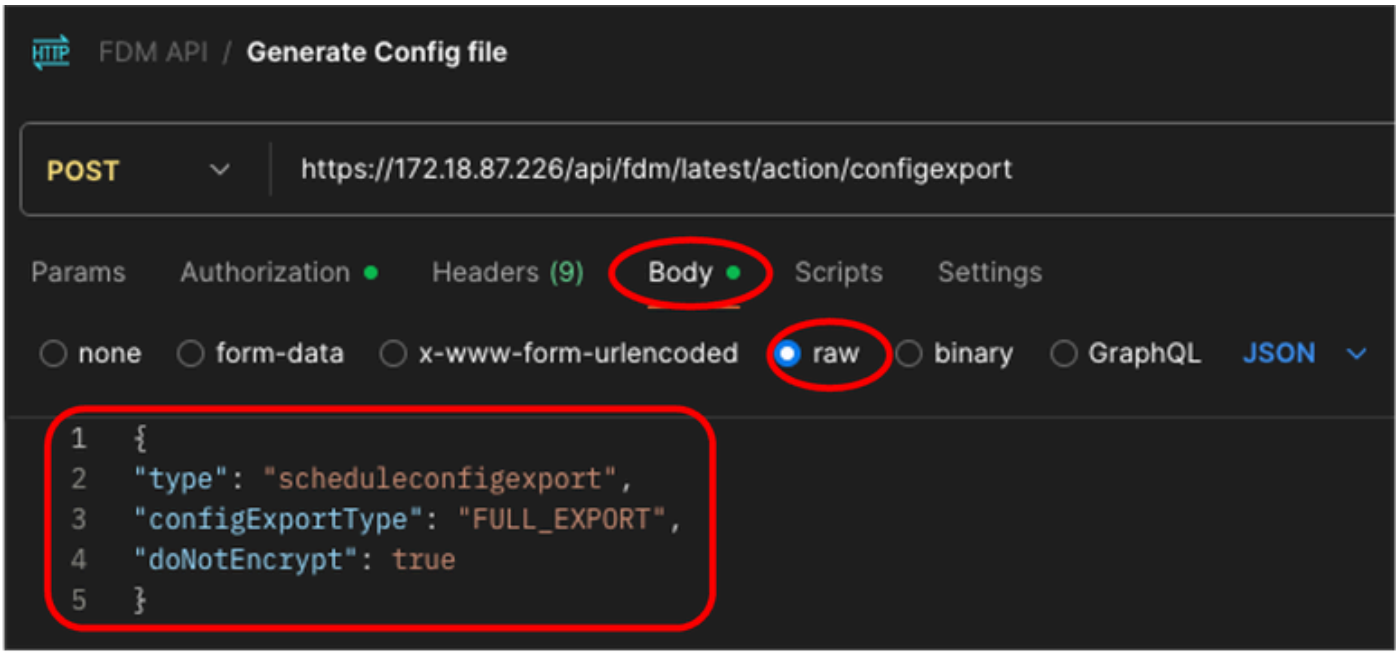
{

「タイプ」:「scheduleconfigexport」、

"configExportType": "FULL_EXPORT",

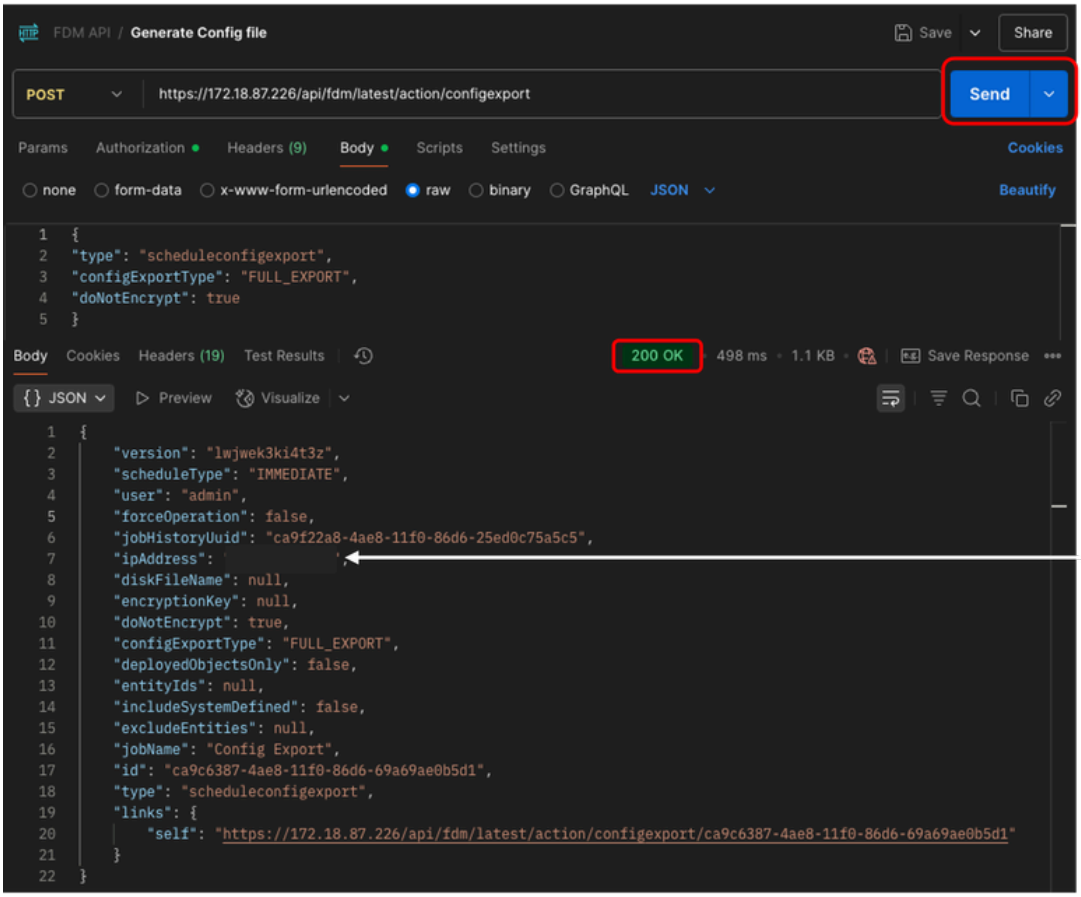
"doNotEncrypt": true

}



Postman – 構成ファイル要求の生成 – 本文

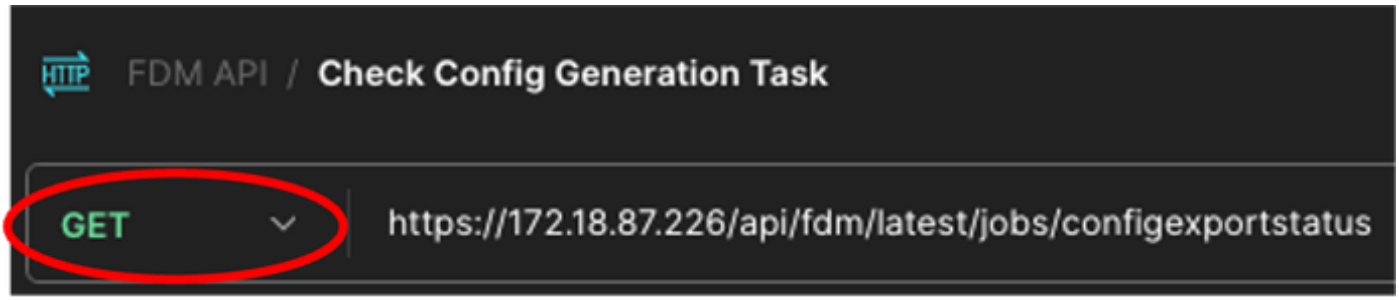
10. 最後に、Sendをクリックします。問題がなければ、200 OKの応答を受信します。



Postman – 構成ファイル要求の生成 – 出力

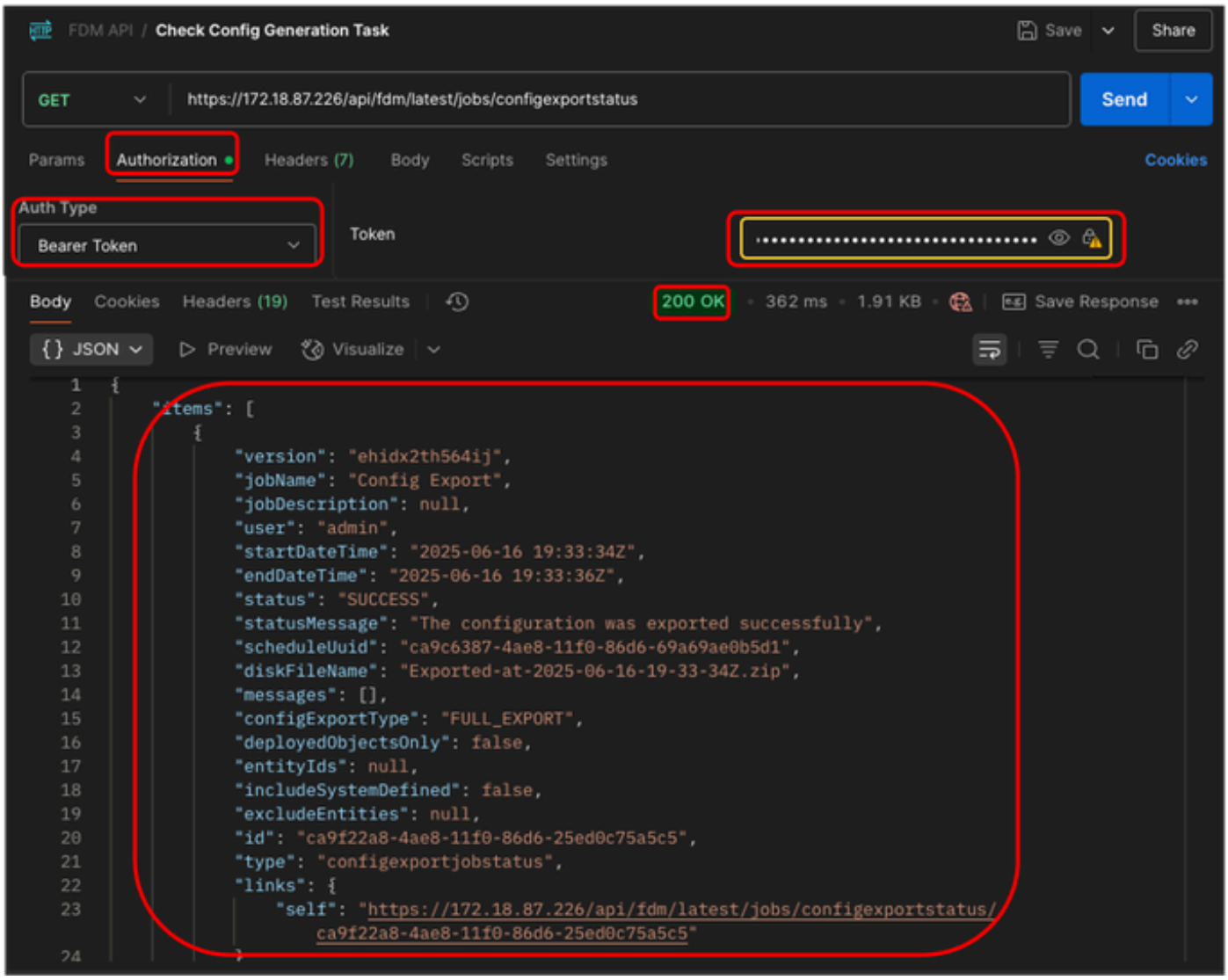
11. ステップ2を繰り返して、新しい要求を作成します。GETは今回は使用します。

12. この新しい要求を「Check Config Generation Task」と呼びます。これはGET要求として作成されます。また、このコマンドを実行するときには、ドロップダウンメニューからGETを選択する必要があります。GETの横のテキストボックスに、次の行https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus



Postman：設定エクスポートステータス要求の確認

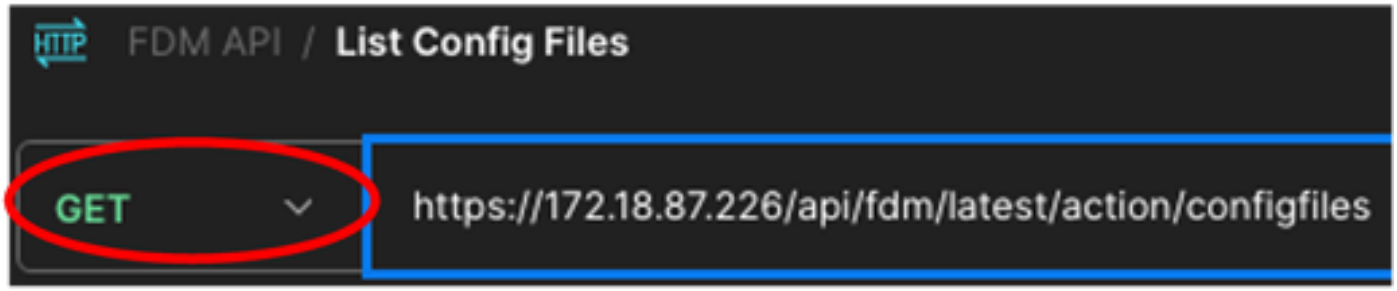
13. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスにステップ5でコピーしたトークンを貼り付けます。最後に、Sendをクリックします。問題がなければ、200 OK応答を受信し、JSONフィールドにタスクのステータスやその他の詳細を表示できます。



Postman:Config Export Status Request：許可および出力

14. ステップ2を繰り返して新しい要求を作成するため、今回はGETを使用します。

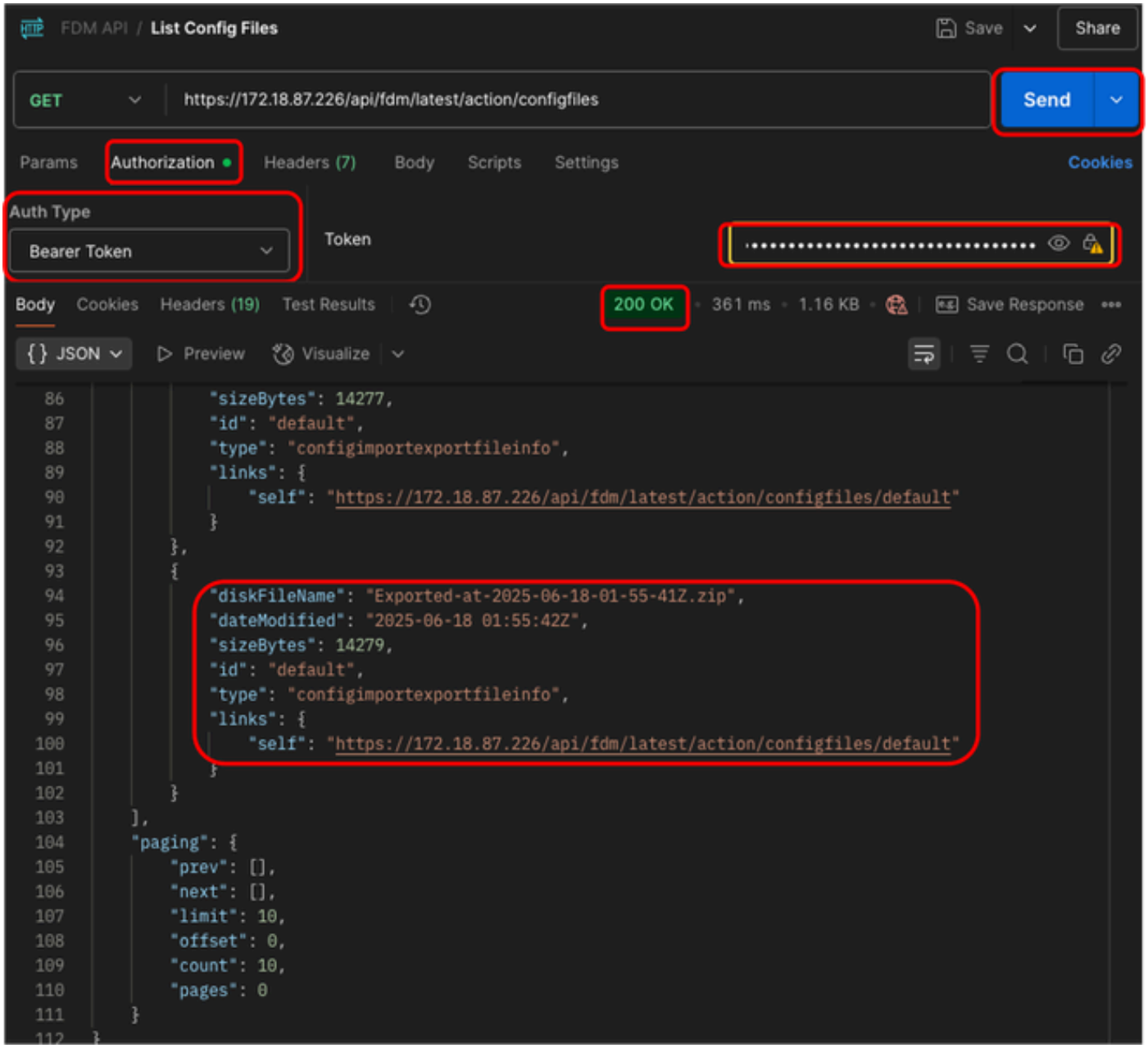
15. この新しい要求を「List Config Files」と呼びます。GET要求はGET要求として作成されますが、この要求を実行する際に、ドロップダウンメニューからGETを選択する必要もあります。GETの横のテキストボックスに、次の行https://<FDM IP ADD>/api/fdm/latest/action/configfilesを挿入します



Postman – エクスポートされた構成ファイルの一覧表示の要求

16. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスにステップ5でコピーしたトークンを貼り付けます。最後に、

Sendをクリックします。 問題がなければ、200 OK応答を受信し、JSONフィールドにエクスポートされたファイルのリストが表示されます。最新のものが下部に表示されます。最新のファイル名（ファイル名のより新しい日付）をコピーします。これは、このファイル名が最後のステップで使用されるためです。



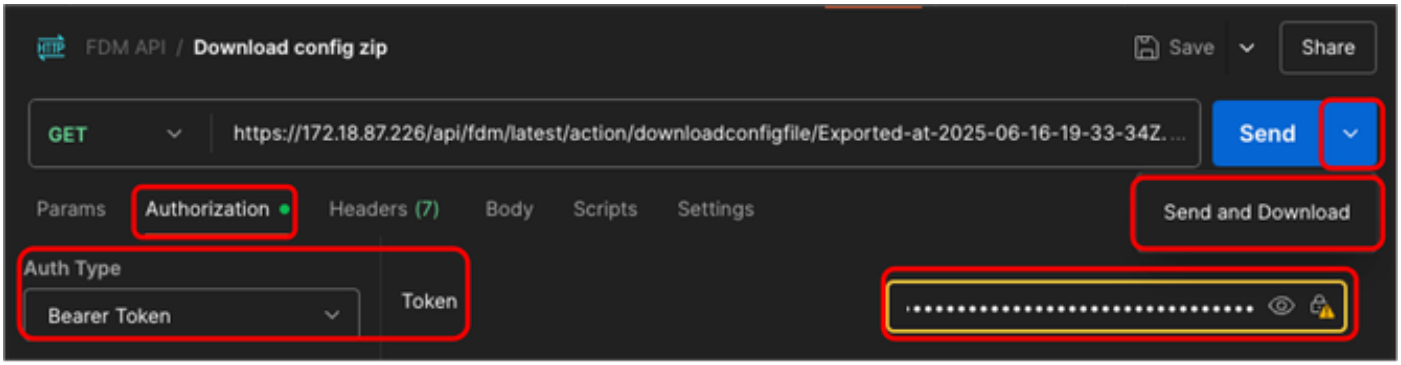
Postman – エクスポートされた設定ファイルの一覧表示リクエスト – 許可と出力

17. ステップ2を繰り返して新しい要求を作成するため、今回はGETを使用します。

18. 次の新しい要求を呼び出します。config zipをダウンロードします。GET要求はGET要求として作成されますが、この要求を実行する際に、ドロップダウンメニューからGETを選択する必要もあります。GETの横のテキストボックスに次の行を挿入し、手順16でコピーしたファイル名を最後に貼り付けます。https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >

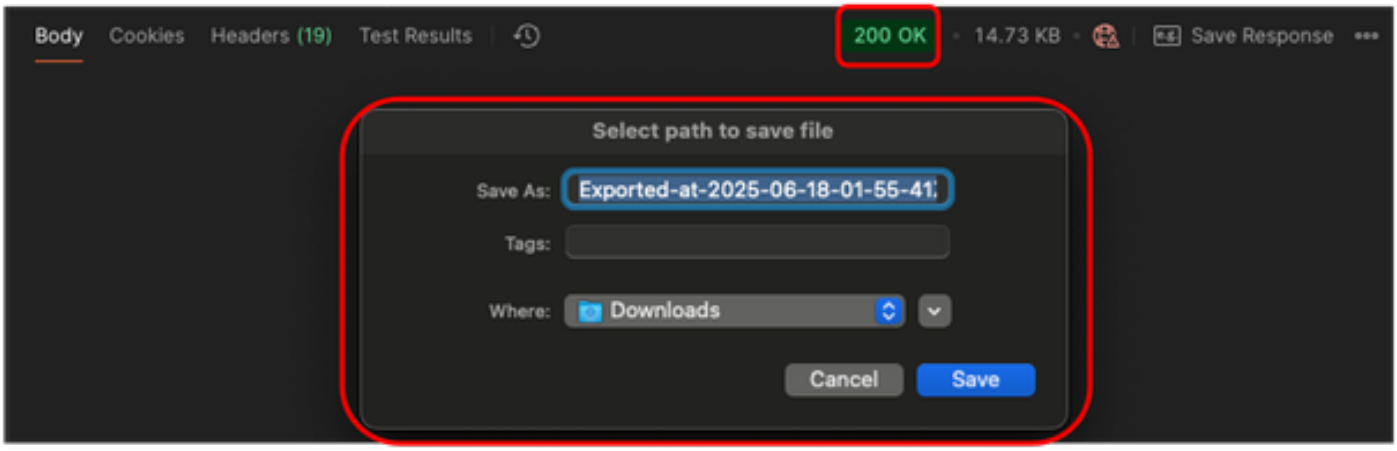
Postman:Config.zipファイル要求のダウンロード

19. Authorizationタブで、ドロップダウンメニューからBearer Token as Auth Typeを選択し、Tokenの横のテキストボックスに、ステップ5でコピーしたトークンを貼り付けます。最後に、Sendの横にある下矢印をクリックして、Send and Downloadを選択します。



Postman - Config.zipファイルのダウンロード要求 – 許可

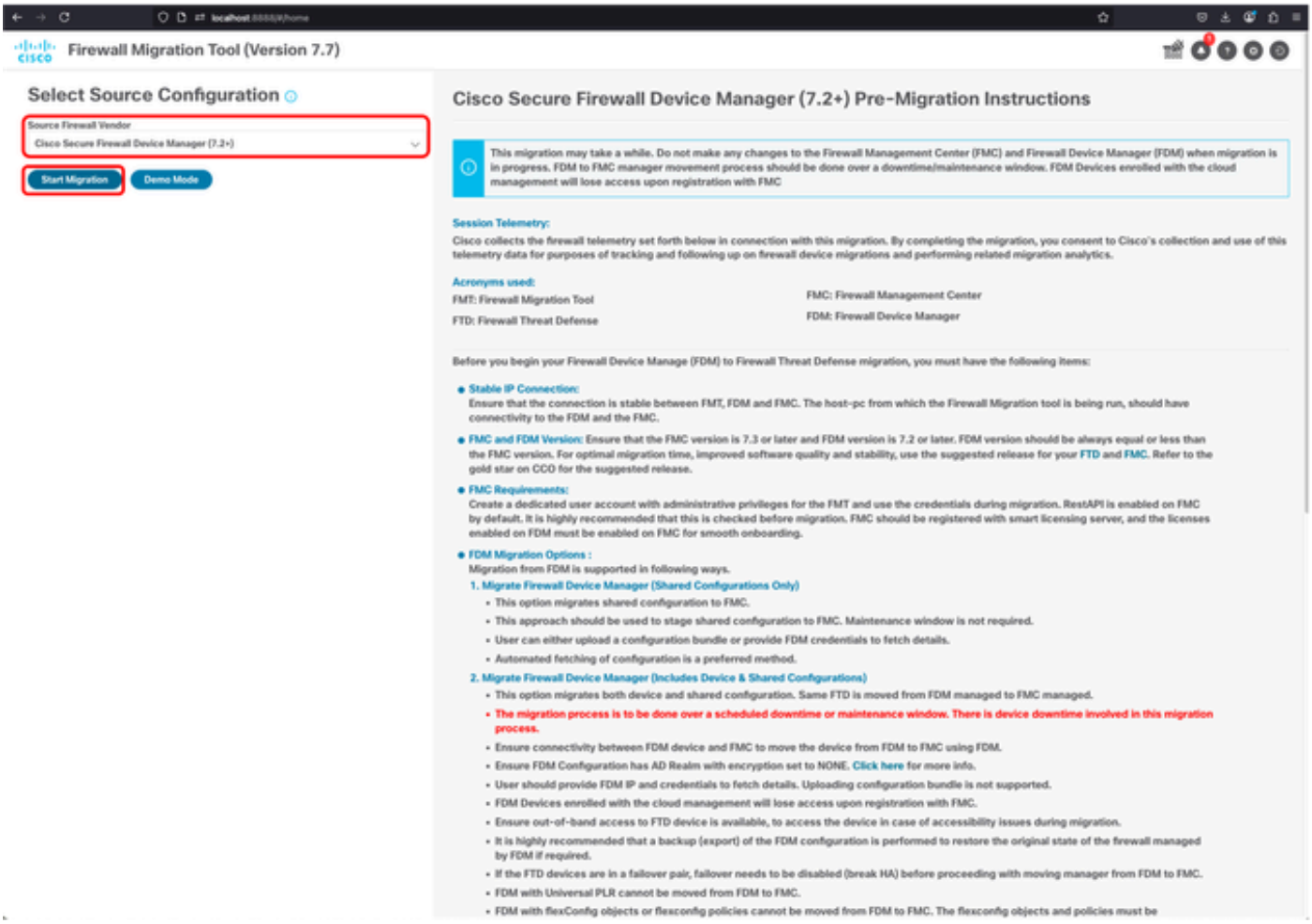
20. 問題がなければ、200 OK応答が表示され、configuration.zipファイルの保存先フォルダを指定するよう求めるポップアップウィンドウが表示されます。これで、この.zipファイルをファイアウォール移行ツールにアップロードできます。



Postman - Config.zipファイルのダウンロード要求 – 保存

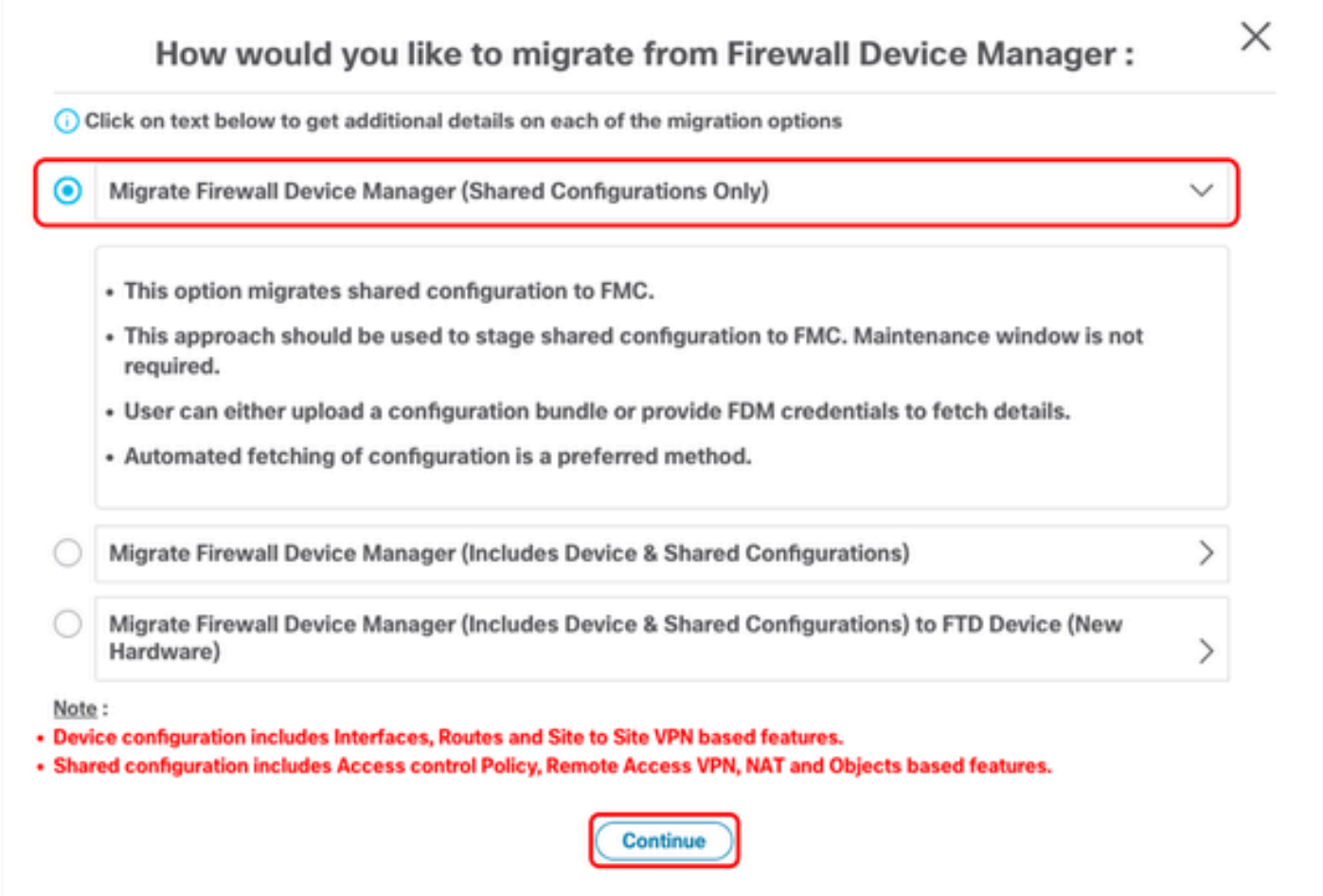
ファイアウォール移行ツール

21. Firewall Migration Toolを開き、Select Source Configurationドロップダウンメニューで、Cisco Secure Firewall Device Manager (7.2+)を選択し、Start Migrationをクリックします。



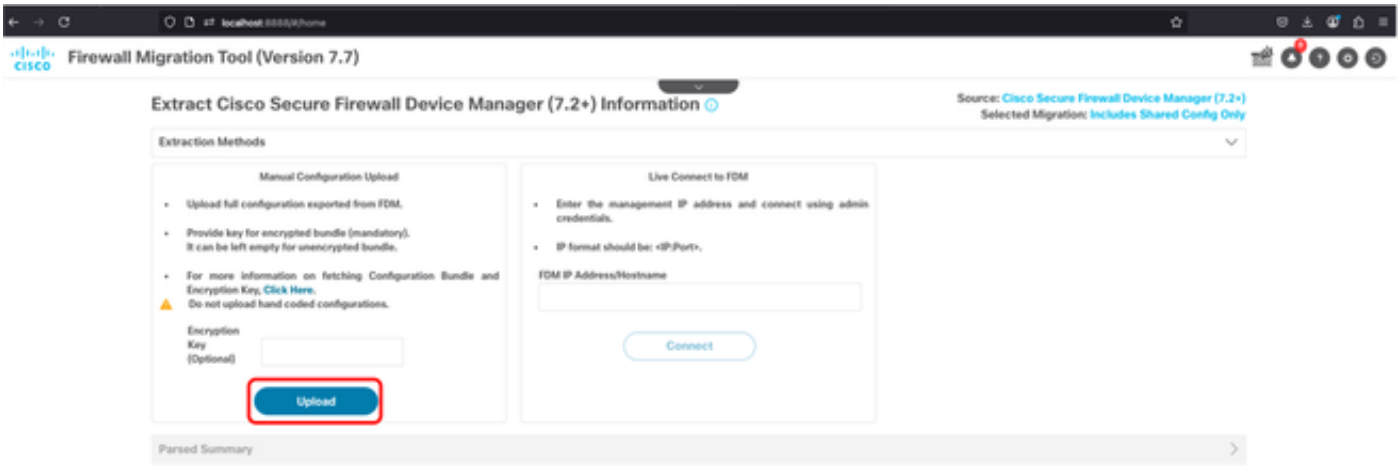
FMT - FDM選択

22. 最初のオプションボタンをチェックし、Migrate Firewall Device Manager (Shared Configurations Only)にチェックマークを入れて、Continueをクリックします。



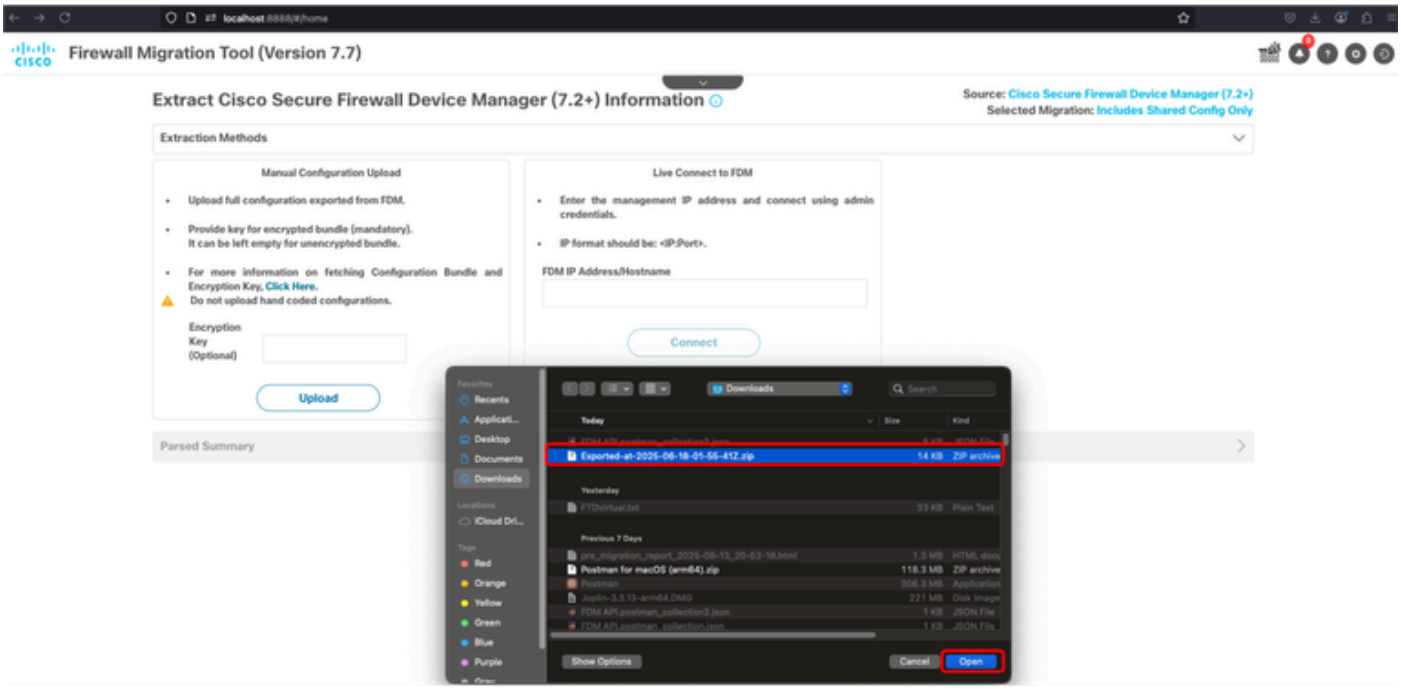
FMT - FDM移行共有構成のみ

23. 左側のパネル(Manual Configuration Upload)でUploadをクリックします。



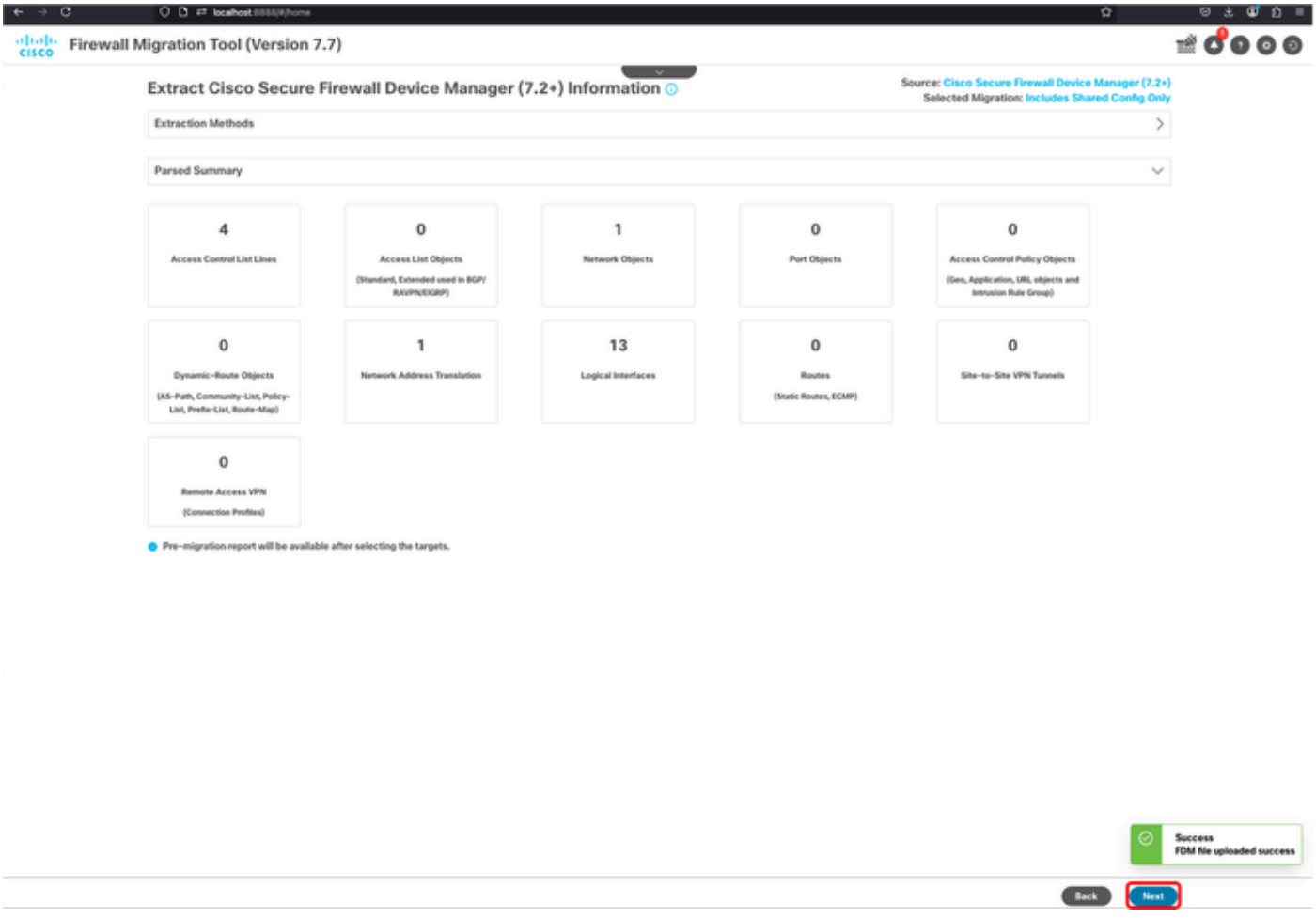
FMT:Config.zipファイルのアップロード

24. 前に保存したフォルダでエクスポートしたzip設定ファイルを選択し、開くをクリックします。



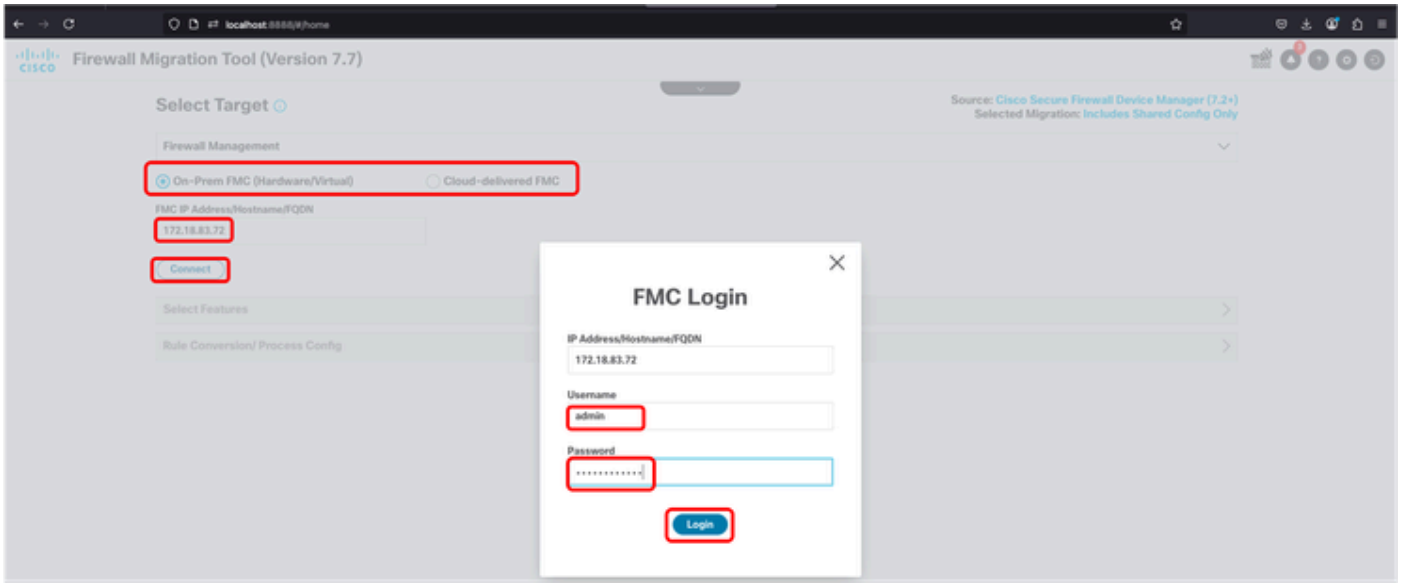
FMT - Config.zipファイルの選択

25. すべてが期待どおりに進んだ場合は、「解析された要約」が表示されます。また、右下隅に、FDMファイルが正常にアップロードされたことを通知するポップアップが表示されます。[Next] をクリックします。



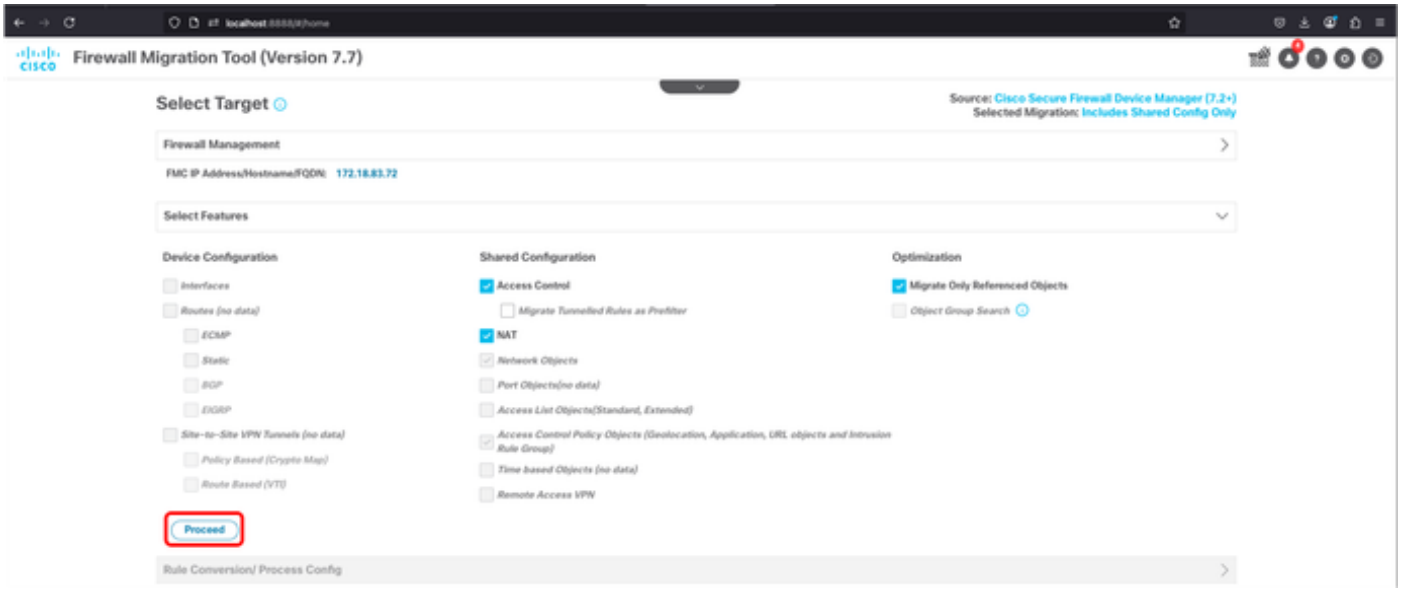
FMT – 解析の概要

26. 環境に適したオプション（オンプレミスFMCまたはCd-FMC）をチェックします。 このシナリオでは、オンプレミスFMCが使用されます。FMC IP addressを入力し、Connectをクリックします。新しいポップアップが表示され、FMCクレデンシャルの入力を求められます。この情報を入力したら、Loginをクリックします。



FMT:FMCターゲット・ログイン

27. 次の画面には、移行されるターゲットFMCと機能が表示されます。[続行（Proceed）] をクリックします。

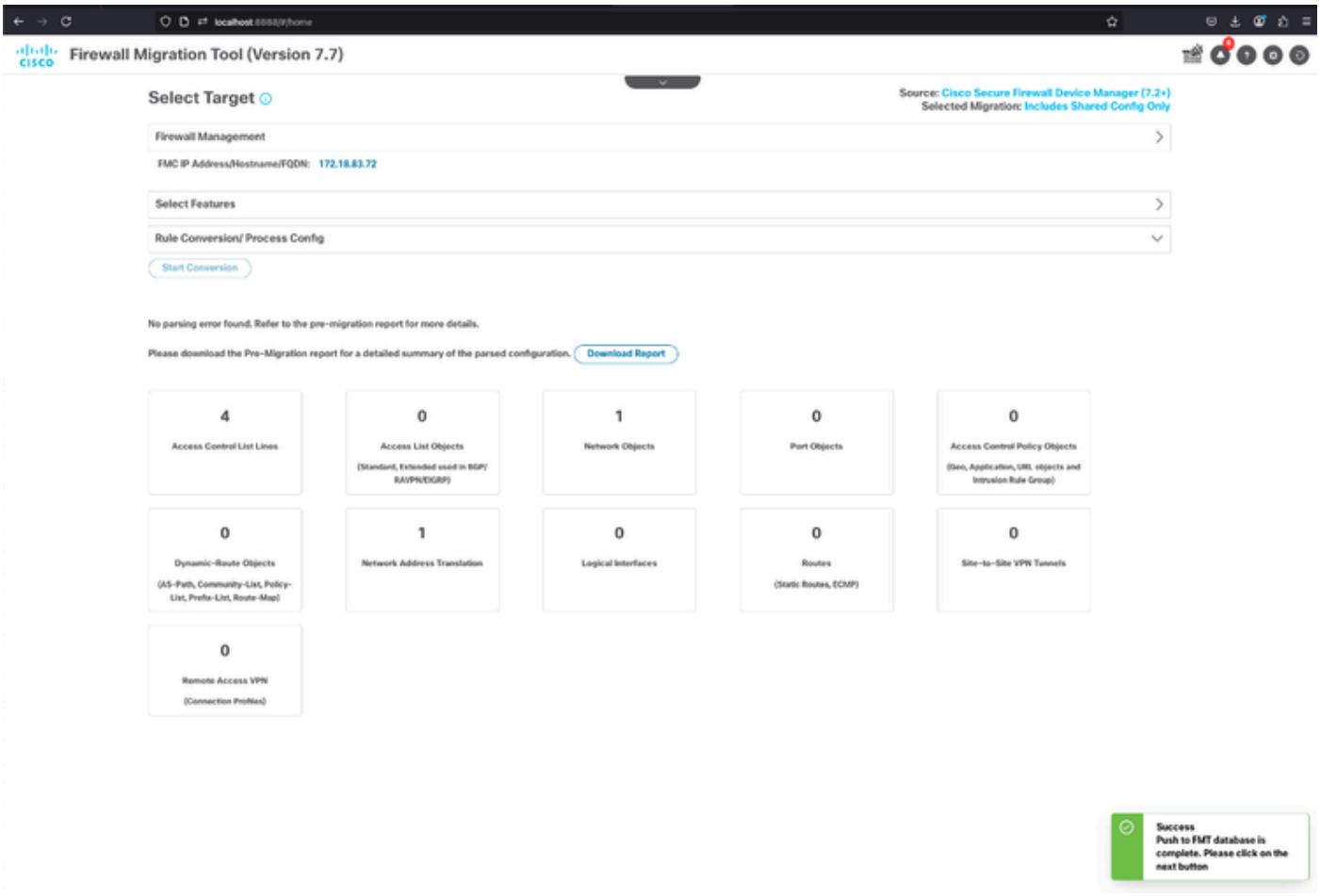


FMT - FMCターゲット – 機能選択

28. FMCターゲットが確定したら、Start Conversionボタンをクリックします。

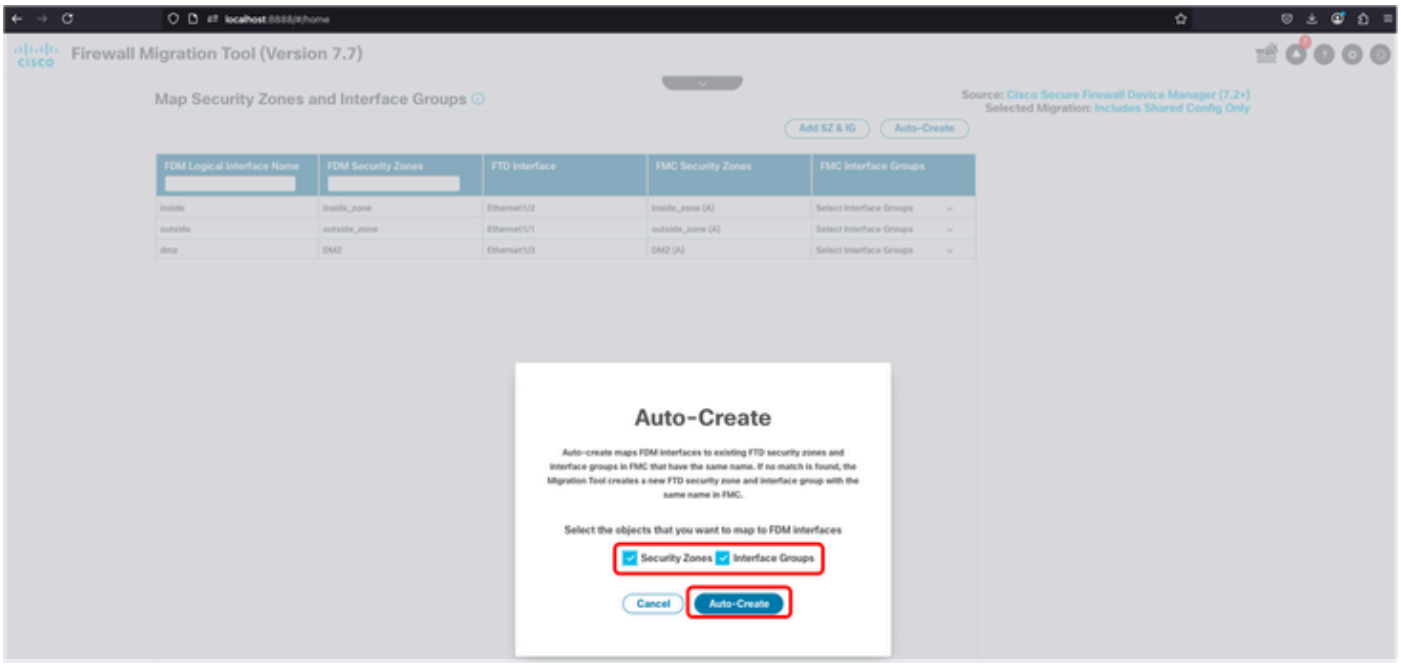
FMT:Config Conversionの開始

29. すべてが正しく行われると、右下にポップアップが表示され、FMTデータベースへのプッシュが完了したことが通知されます。[Next] をクリックします。



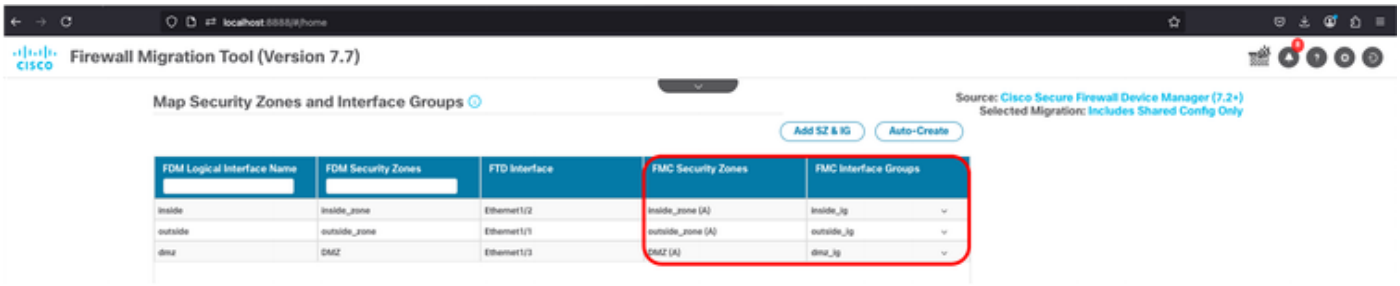
FMT – データベースのプッシュが正常に完了しました

30. 次の画面で、手動で作成するか、またはセキュリティゾーンとインターフェイスグループの自動作成を選択する必要があります。このシナリオでは、auto-createが使用されます。



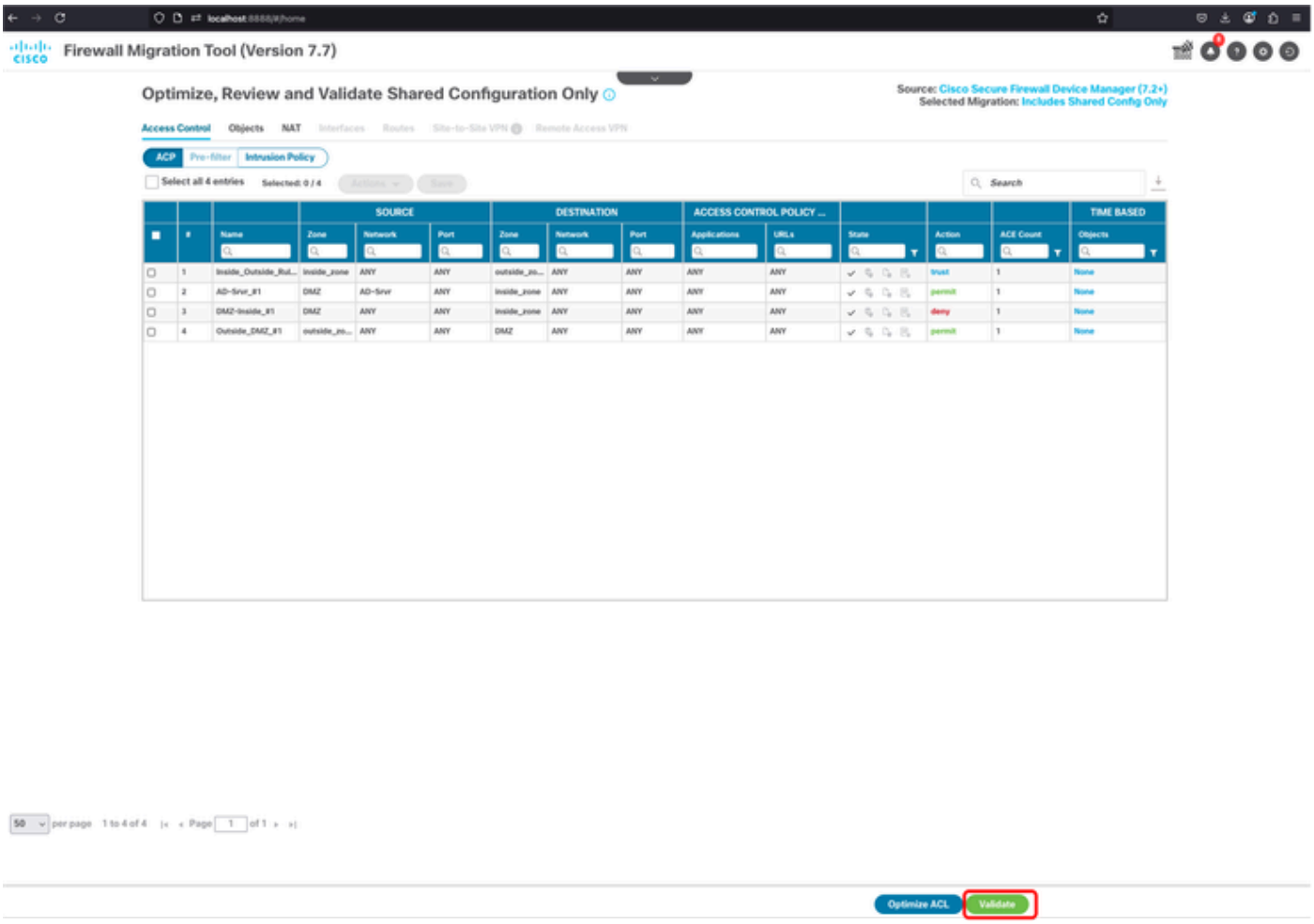
FMT:Auto Creating Security Zones and Interface Groups（セキュリティゾーンおよびインターフェイスグループの自動作成）

31. 完了すると、表の4列目と5列目に、それぞれセキュリティゾーンとインターフェイスグループが表示されます。



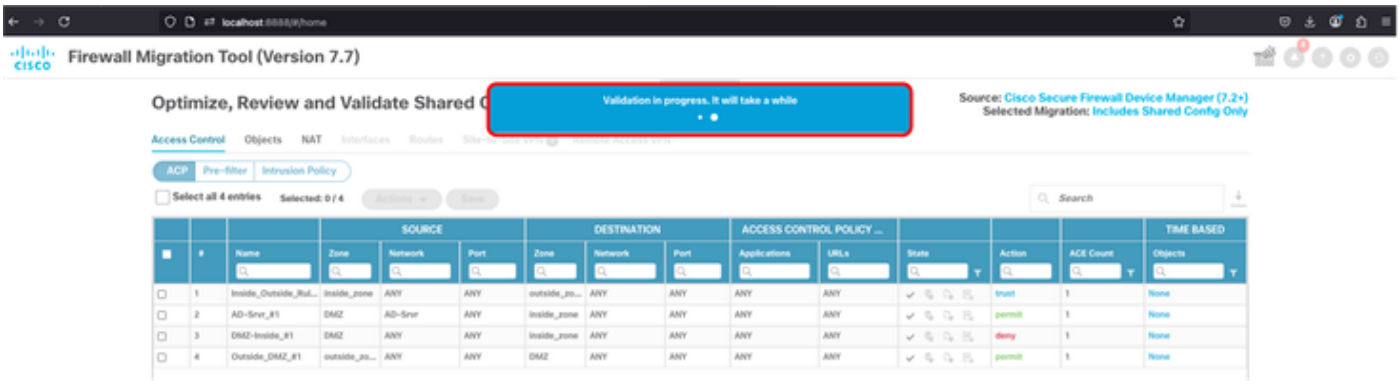
FMT：セキュリティゾーンとインターフェイスグループが正常に作成されました

32. 次の画面では、ACLを最適化するか、ACP、オブジェクト、およびNATを検証できます。完了したら、Validateボタンをクリックします。



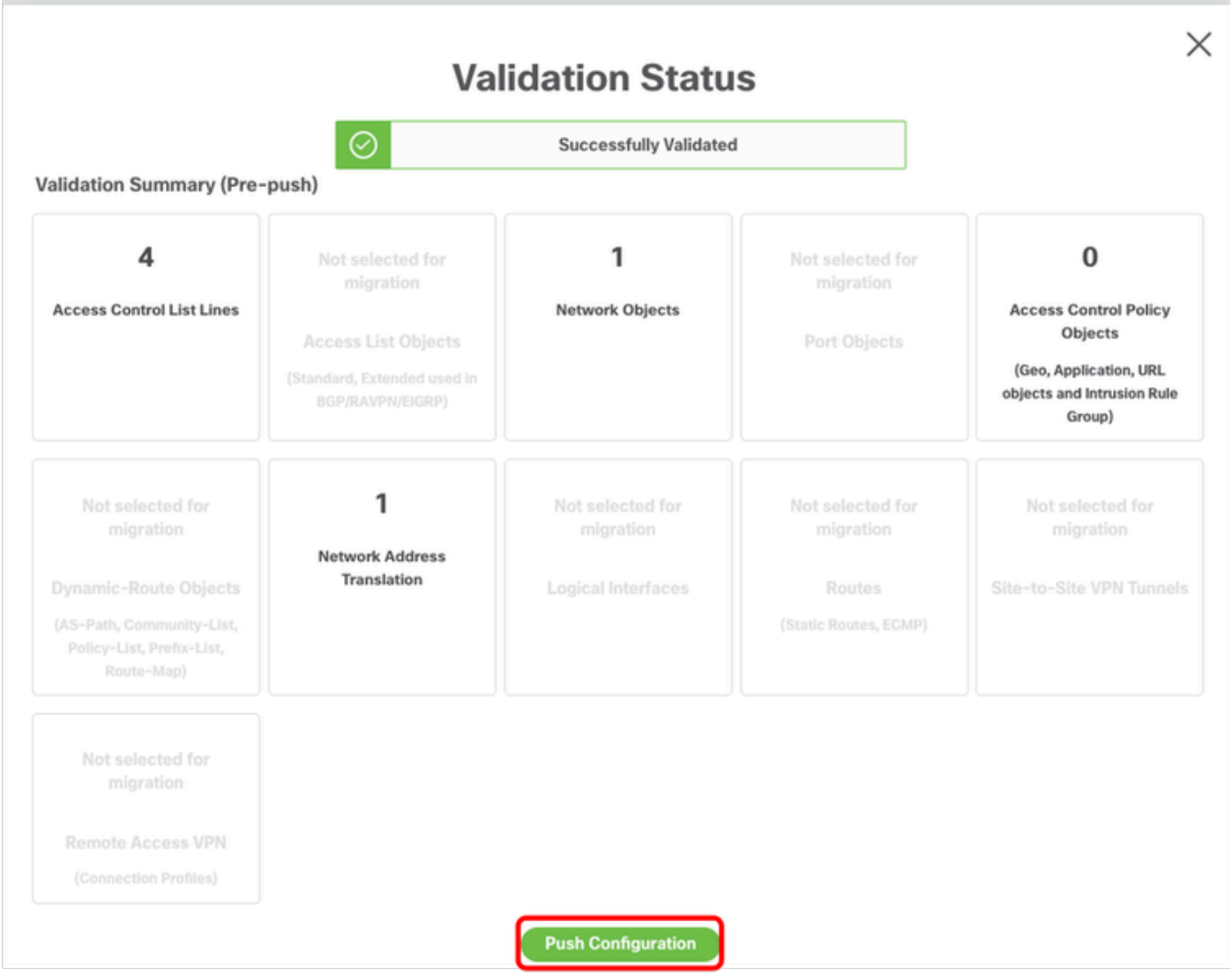
FMT:ACLの最適化：移行の検証

33. 検証が完了するまで数分かかります。



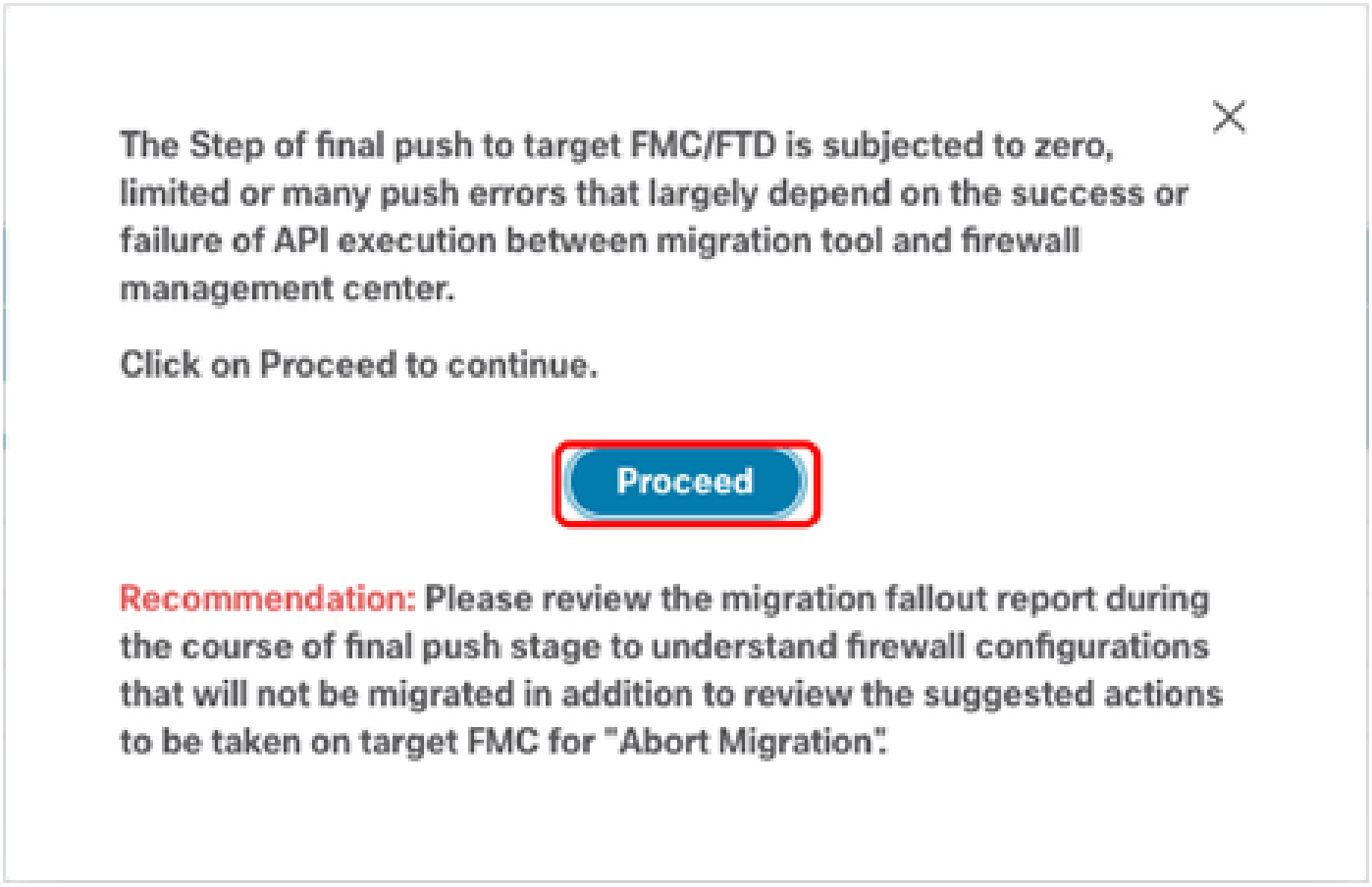
FMT:Validation in Progress（検証中）

34. 設定が完了すると、FMTによって設定が正常に検証されたことが通知され、次のステップとしてPush Configurationボタンをクリックします。



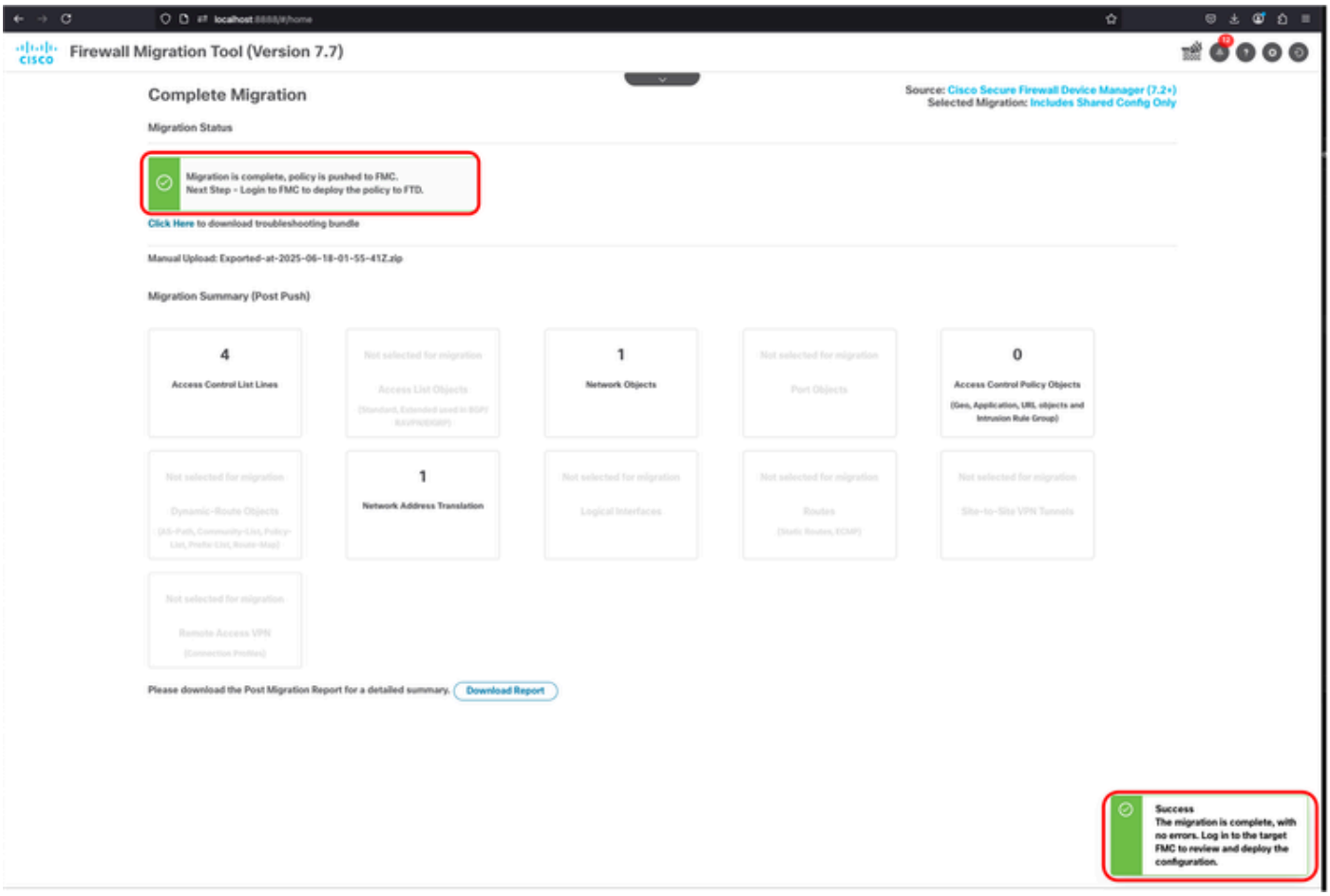
FMT – 検証に成功しました – 構成をFMCにプッシュします

35. 最後に、Proceedボタンをクリックします。



FMT – 構成プッシュの続行

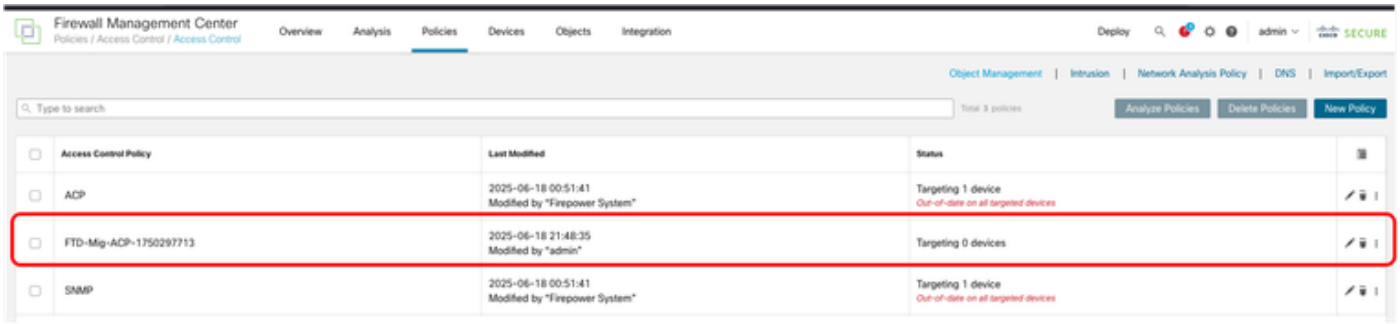
36. すべてが期待どおりに進んだ場合は、「Migration succeeded」通知が表示されます。FMTから、FMCにログインして、移行したポリシーをFTDに展開するように求められます。



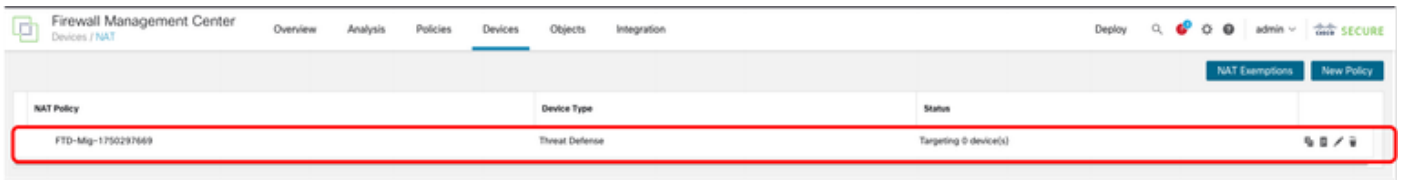
FMT:Migration Succeeded通知

FMCの検証

37. FMCにログイン後、ACPおよびNATポリシーがFTD-Migとして表示されます。これで、新しいFTDの導入に進むことができます。



FMC:ACPの移行



FMC:NATポリシーの移行

関連情報

- FMT - FDMからFMCへの移行ガイド
- FMTリリースノート

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。